

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
Three (3) Subject Digital Devices, more fully
described in Attachment A.

Case No. MJ23-573

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Three (3) Subject Digital Devices, more fully described in Attachment A.

located in the _____ Western _____ District of _____ Washington _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252(a)(2),(b)(2)	Possession of Child Pornography

The application is based on these facts:

- ☒ See Affidavit of Special Agent Shafqat Mirza, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

SHAFQAT M MIRZA

Digitally signed by SHAFQAT M
MIRZA
Date: 2023.11.29 09:17:34 -08'00'

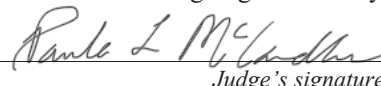
Applicant's signature

Shafqat Mirza, Special Agent (HSI)

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 11/30/2023


Judge's signature

City and state: Seattle, Washington

Paula L. McCandlis, United States Magistrate Judge

Printed name and title

AFFIDAVIT OF SAFQAT MIRZA

STATE OF WASHINGTON)
) SS
COUNTY OF KING)

I, Shafqat Mirza, a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations (HSI), Seattle, Washington, having been duly sworn, state as follows:

AFFIANT BACKGROUND

I am a Special Agent with the U.S. Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the Special Agent in Charge (SAC), Seattle, Washington. As a Special Agent (SA) with the HSI and a law enforcement officer of the United States, I am authorized by law to conduct investigations and to make arrests for felony and administrative offenses. I have been employed as a federal law enforcement officer since 2002, as an HSI Special Agent since 2006, and at HSI Seattle, WA since July 2021. I have extensive training and experience in several areas of investigation, but for the purposes of this complaint, I have specific training and experience related to investigations and offenses involving child exploitation, child pornography, and child sex trafficking. HSI is responsible for enforcing the customs and immigration laws and federal criminal statutes of the United States.

As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I am a graduate of the Federal Law Enforcement Training Center (FLETC), ICE Special Agent Training Program, and have received further specialized training in investigating child

1 pornography and child exploitation crimes. I have also had the opportunity to observe
2 and review examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have
3 participated in the execution of previous search warrants, which involved child
4 exploitation and/or child pornography offenses, and the search and seizure of computers,
5 related peripherals, and computer media equipment. I am a member of the Seattle
6 Internet Crimes Against Children Task Force (ICAC), and work with other federal, state,
7 and local law enforcement personnel in the investigation and prosecution of crimes
8 involving the sexual exploitation of children.

9 INTRODUCTION AND PURPOSE OF AFFIDAVIT

10 1. The facts in this affidavit come from my personal observations, my training
11 and experience, and information obtained from other agents and witnesses. This affidavit
12 is intended to show merely that there is sufficient probable cause for the requested
13 warrants and does not set forth all of my knowledge about this matter. Based on my
14 training and experience and the facts as set forth in this affidavit, there is probable cause
15 to believe that violations of Title 18 United States Code Sections 2252(a)(4), (b)(2),
16 Possession of Child Pornography have been committed by **BRETT GILLETTE**. There
17 is also probable cause to search the following devices: (1) a blue colored Samsung
18 Galaxy S20, Model: SM-G781U; (2) a black colored Samsung Galaxy S21, Model: SM-
19 G990U; and (3) a black colored Samsung Galaxy S9 (hereafter SUBJECT DIGITAL
20 DEVICES) for evidence of these crimes and contraband or fruits of these crimes, as
21 described in Attachment B.

22 DEFINITIONS

23 The following definitions apply to this affidavit:

24 1. “Chat,” as used herein, refers to any kind of text communication over the
25 internet that is transmitted in real-time from sender to receiver. Chat messages are
26 generally short in order to enable other participants to respond quickly and in a format
27

1 that resembles an oral conversation. This feature distinguishes chatting from other text-
2 based online communications such as internet forums and email.

3 2. For the purposes of this affidavit, a “minor” refers to any person less than
4 eighteen years of age and for the purpose of this search warrant, “Child pornography,” as
5 used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit
6 conduct where (a) the production of the visual depiction involved the use of a minor
7 engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer
8 image, or computer-generated image that is, or is indistinguishable from, that of a minor
9 engaged in sexually explicit conduct, or (c) the visual depiction has been created,
10 adapted, or modified to appear that an identifiable minor is engaged in sexually explicit
11 conduct).

12 3. “Sexually explicit conduct” means actual or simulated (a) sexual
13 intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons
14 of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic
15 abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18
16 U.S.C. § 2256(2).

17 4. “Cloud-based storage service,” as used herein, refers to a publicly
18 accessible, online storage provider that collectors of depictions of minors engaged in
19 sexually explicit conduct can use to store and trade depictions of minors engaged in
20 sexually explicit conduct in larger volumes. Users of such a service can share links and
21 associated passwords to their stored files with other traders or collectors of depictions of
22 minors engaged in sexually explicit conduct in order to grant access to their collections.
23 Such services allow individuals to easily access these files through a wide variety of
24 electronic devices such as desktop and laptop computers, mobile phones, and tablets,
25 anywhere and at any time. An individual with the password to a file stored on a cloud-
26 based service does not need to be a user of the service to access the file. Access is free
27 and readily available to anyone who has an internet connection.

1 5. “Computer,” as used herein, refers to “an electronic, magnetic, optical,
2 electrochemical, or other high speed data processing device performing logical or storage
3 functions, and includes any data storage facility or communications facility directly
4 related to or operating in conjunction with such device,” including smartphones and
5 mobile devices.

6 6. “Data,” as used herein refers to the quantities, characters, or symbols on
7 which operations are performed by a computer, being stored and transmitted in the form
8 of electrical signals and recorded on magnetic, optical, or mechanical recording media.

9 7. “Digital Devices” as used herein refers to any physical object that has a
10 computer, microcomputer, or hardware that is capable of receiving, storing, possessing,
11 or potentially sending data.

12 8. “Internet Service Providers” (“ISPs”), as used herein, are commercial
13 organizations, community-owned, non-profit, or otherwise privately-owned companies
14 that are in business to provide individuals and businesses access to the internet. ISPs
15 provide a range of functions for their customers including access to the internet, web
16 hosting, e-mail, remote storage, and co-location of computers and other communications
17 equipment.

18 9. “Mobile applications,” as used herein, are small, specialized programs
19 downloaded onto mobile devices that enable users to perform a variety of functions,
20 including engaging in online chat, reading a book, or playing a game.

21 10. “Records,” “documents,” and “materials,” as used herein, include all
22 information recorded in any form, visual or aural, and by any means, whether in
23 handmade, photographic, mechanical, electrical, electronic, or magnetic form.

24 11. “User Attributes,” as used herein refers to any tangible data, documents,
25 settings, programs, or other information that provides information related to the identity
26 of the specific user of the device, computer, application, program, or record.

27 //

SUMMARY OF PROBABLE CAUSE

12. On or about August 18, 2011, Brett Allen GILLETTE (hereafter GILLETTE), was arrested for the violation of Child Molestation in the First Degree, in Clark County, Washington. On February 13, 2012, GILLETTE plead guilty to Child Molestation in the First Degree in the Clark County Superior Court and was sentenced to a minimum term of sixty-two months to the maximum term of lifetime on March 30, 2012. GILLETTE was committed to the Washington State Department of Corrections (DOC) and released from prison on November 29, 2017, at which time community custody commenced which included both standard and special conditions of supervision. Specifically, GILLETTE was precluded from possessing electronic devices unless authorized by his assigned Community Corrections Officer (CCO).

13. On or about September 6, 2023, GILLETTE reported to the DOC Bellevue Field Office as directed pursuant to the terms of community custody. GILLETTE submitted to a polygraph examination conducted by polygraph examiner Rick Minnich. GILLETTE failed the examination pertaining to accessing/viewing sexually explicit material/pornography and Mr. Minnich disclosed this failure to GILLETTE's CCO. Based on this notification, a request to physically search GILLETTE's residence, property, and electronic devices for sexually explicit material was approved by Community Corrections Supervisor (CCS) Christopher Duran. A DOC CCO conducted a manual search of an approved iPhone and no evidence of any sexually explicit material was recovered. GILLETTE previously reported to DOC CCO's verbally and in writing on a social media and Electronic Monitoring Agreement that he did not possess or own any other internet capable devices.

14. On or about September 6, 2023, CCOs Erin Rylands, Ryan Thomas, and Mohammad Khatibi arrived at GILLETTE's DOC approved residence located on

1 Eastgate Way, Bellevue, Washington.¹ GILLETTE had been assigned to and resided in
2 bed # 17. GILLETTE initially informed the CCOs that he did not have assigned storage
3 space at the shelter aside from the locker next to his bed, which was not located where it
4 was supposed to be. GILLETTE claimed that he did not keep any property at the shelter.
5 An employee of the shelter, Jose Medrano, advised the CCOs that GILLETTE was
6 assigned storage locker #17 which was located in a nearby hallway at the shelter.

7 15. The CCOs then searched GILLETTE's locker # 17 and located the
8 following items: (1) a blue colored Samsung Galaxy S20 Model SM-G781U; (2) a black
9 colored Samsung Galaxy S21 Model: SM-G990U; (3) a black colored Samsung Galaxy
10 S9+; (4) multiple documents under GILLETTE's name to include legal documents; and
11 (4) a backpack which GILLETTE identified as his property. GILLETTE then admitted to
12 storing his personal property in the locker and to lying because he did not want CCOs to
13 seize his property. GILLETTE denied owning the above listed three smart phones (the
14 SUBJECT DIGITAL DEVICES).

15 16. CCO Rylands was assigned GILLETTE's case for further investigation.
16 On or about September 6, 2023, CCO Rylands returned the SUBJECT DIGITAL
17 DEVICES to the DOC Office and charged the SUBJECT DIGITAL DEVICES. CCO
18 Rylands discovered that two of the three SUBJECT DIGITAL DEVICES were already
19 fully charged. One appeared to be damaged and unable to power on. CCO Rylands
20 asked GILLETTE to provide the passwords (i.e. the swipe patterns) to the SUBJECT
21 DIGITAL DEVICES in order to access and manually search for contraband. GILLETTE
22 claimed he did not know the password/swipe pattern to any of the SUBJECT DIGITAL
23 DEVICES. Notably, GILLETTE is required by his safety plan and Social Media and
24 Device Monitoring Electronic Agreement to provide passwords to any electronic devices
25 as a condition to possessing any electronic devices. GILLETTE was booked into SCORE
26

27 ¹ GILLETTE resided at a homeless shelter at the time of the search.

1 Jail by CCO Khatibi for the supervision violations of unauthorized possession of internet
2 capable devices and failing to submit to a search by failing to provide the passwords to
3 the SUBJECT DIGITAL DEVICES.

4 17. On or about September 14, 2023, CCO Rylands transported the SUBJECT
5 DIGITAL DEVICES to Homeland Security Investigations (HSI) forensic laboratory in
6 Seattle, Washington and requested HSI to process the SUBJECT DIGITAL DEVICES to
7 allow CCO Rylands to determine if GILLETTE violated his condition prohibiting him
8 from possessing/viewing sexually explicit material. HSI Computer Forensic Agent
9 (CFA) Alan Heng assisted with the request.

10 18. On or about September 18, 2023, search of the SUBJECT DIGITAL
11 DEVICES was resumed by CCO Rylands and CFA Heng. Using HSI forensic software,
12 CFA Heng was able to locate the password for the Samsung Galaxy S20, Model: SM-
13 G781U cellphone, but was unable to locate the password for the Samsung Galaxy S21,
14 Model: SM-G990U. CFA Heng was unable to access the Samsung Galaxy S9+ because
15 it was damaged.

16 19. In a criminal incident report, dated October 18, 2023, CCO Rylands
17 documented that during the search of the Samsung Galaxy S20, Model: SM-G781U
18 cellphone, Child Sexual Abuse Materials (CSAM), depicting minors engaged in sexually
19 explicit conduct, were located, and described them as follows:

20 a. A video depicting a small boy appearing approximately 4 - 5 years
21 old with his mouth on a man's penis. The male appeared to be a minor due to his small
22 frame. The boy's head was approximately the size of the male's hand on the boy's head.
23 This comparison shows how small the minor male was in comparison to the adult male in
the video.

24 b. A video of a small female, appearing approximately about 4 - 5
25 years old, with a male's penis inserted into her vagina. The female appeared to be a minor
26 based on her small frame, lack of muscle definition, lack of breast development, and
youthful looking facial features.

20. The current terms of GILLETTE's safety plan and Social Media and Device Monitoring Electronic Agreement allows for the use of email on DOC approved devices only. CCO Rylands observed email communications address to GILLETTE on GILLETTE's Samsung Galaxy S20, Model: SM-G781U cellphone. CCO Rylands described the email message preview as follows:

a. May 24, 2023: An email from Chase Bank with the following message preview: "(Cardholder perk) Brett Gillette, your eligible to ... ,".

b. May 24, 2023: And an email from no-reply with the following message preview: "Your Dishwasher Schedule for [6/11/23- 6/17/23 has been... BRETT, At 5/24/23 3:22 PM your Dishwasher schedule (su...".

21. On or about September 18, 2023, CCO Rylands provided the facts of the investigation via a Washington State Department of Corrections Board-Notice of Violation report and requested assistance in a possible prosecution of GILLETTE for the violation of Title 18, United States Code, Section 2252(a)(4)(B), (b)(2). Though I reviewed the forensic examination of GILLETTE's Samsung Galaxy S20, Model: SM-G781U cellphone, I am relying solely on the descriptions of files provided by CCO Rylands for purposes of establishing probable cause to search the SUBJECT DIGITAL DEVICES utilizing any and all forensic capabilities within the Department of Homeland Security Investigation.

22. Because this Application is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation. I have set forth only the facts I believe are relevant to the determination of probable cause to believe evidence, fruits, and instrumentalities of violations of Title 18 United States Code Sections 2252(a)(2),(b)(2) Possession of Child Pornography will be found in or within the SUBJECT DIGITAL DEVICES.

TECHNICAL BACKGROUND

23. Courts have recognized that the majority of Americans possess and use cellular telephones, and that most of those keep the phones within their reach at all times.

1 Cellular telephones are used for, among other things, voice, text, email, and SMS
2 communications; accessing and posting to social networking websites, surfing the
3 internet, taking, and storing photographs, creating, and storing documents, notes, music,
4 mapping directions to places, etc. Courts have recognized that these devices “smart
5 phones” are essentially small computers with vast storage capacities. Information deleted
6 by the user can be recovered, years after deletion, upon examination of a cell phone’s
7 data.

8 24. Based on my training and experience, I know that the development of
9 computers and portable digital devices in general have revolutionized the way in which
10 those who seek out depictions of minors engaged in sexually explicit conduct are able to
11 obtain this material. Computers serve four basic functions in connection with depictions
12 of minors engaged in sexually explicit conduct: production, communication, distribution,
13 and storage. Additionally, I know that the computer’s capability to store images in digital
14 form makes it an ideal repository for depictions of minors engaged in sexually explicit
15 conduct. The size of the electronic storage media (often referred to as a “hard drive”)
16 used in home computers has grown tremendously within the last several years. Hard
17 drives with the capacity of terabytes are not uncommon. These drives can store
18 thousands of images and/or videos at a high resolution.

19 25. Based on my training and experience and information provided to me by
20 electronic forensic detectives and agents, I know that data can quickly and easily be
21 transferred from one digital device to another digital device via messages, apps, file
22 sharing etc., and via a USB cable or other wired connection. Data can be transferred
23 from computers or other digital devices to internal and/or external hard drives, tablets,
24 mobile phones, and other mobile devices via a USB cable or other wired connection.
25 Data can also be transferred between computers and digital devices by copying data to
26 small, portable data storage devices including USB (often referred to as “thumb”) drives,
27 memory cards (Compact Flash, SD, microSD, etc.) and memory card readers, and optical
discs (CDs/DVDs).

1 26. Based on my training and experience, collectors and distributors of
2 depictions of minors engaged in sexually explicit conduct also use online, remote,
3 resources to retrieve and store depictions of minors engaged in sexually explicit conduct,
4 including services offered by companies such as Google, Yahoo, Apple, Amazon, and
5 Dropbox, among others. The online services allow a user to set up an account with a
6 remote computing service that provides email services and/or electronic storage of
7 electronic files in any variety of formats. A user can set up, and access, an online storage
8 account from any digital device with access to the Internet. Evidence of such online
9 storage of depictions of minors engaged in sexually explicit conduct is often located on
10 the user's computer or smart phone.

11 27. Based on my training and experience, communications by way of a
12 computer/smart device can be saved or stored on the computer/smart device used for
13 these purposes. Storing this information can be intentional, i.e., by saving an email or
14 saving the location of one's favorite websites in, for example, "bookmarked" files.
15 Digital information can also be retained unintentionally, e.g., traces of the path of an
16 electronic communication may be automatically stored in many places (e.g., temporary
17 files or ISP client software, among others). Examples of this stored data include user-
18 created or saved data, such as contact lists, messages sent and received, images, audio
19 and video files, personal calendars, notes, prescriptions, bank statements, videos,
20 documents, and images; as well as device-generated data, such as user identity
21 information, passwords, usage logs and information pertaining to the physical location of
22 the device over time. Examples of data stored in a smart phone that can reveal a person's
23 location at specific dates and times include metadata and EXIF tags associated with
24 photographs; IP addresses, which are associated with a geographic location; and
25 geographic location associated with the phone sending/receiving signals with cell towers
26 and satellites. As such, a person's use of the smart phone can reveal where a person has
27 been at dates and times relevant to the crime(s) under investigation; a person's activity at
relevant dates and times, and/or places a person frequents at which that person is likely to
be found for arrest or at which the suspect stored or inadvertently left evidence behind.

1 28. In addition to electronic communications, a user's Internet activities
2 generally leave traces or "footprints" and history files of the browser application used. A
3 forensic examiner often can recover evidence suggesting whether a computer/smart
4 device was using a specific website or application, and when certain files under
5 investigation were uploaded or downloaded. Such information is often maintained
6 indefinitely until overwritten by other data. Additionally, even if such information is
7 deleted from the memory or storage of the device the data may reside on the device for an
8 extended period of time until overwritten by the operating system of the device.

9 29. Based on my training and experience, I have learned that in addition to the
10 traditional collector, law enforcement has encountered offenders who obtain depictions of
11 minors engaged in sexually explicit conduct from the internet, view the contents and
12 subsequently delete the contraband, often after engaging in self-gratification. In light of
13 technological advancements, increasing Internet speeds and worldwide availability of
14 child sexual exploitative material, this phenomenon offers the offender a sense of
15 decreasing risk of being identified and/or apprehended with quantities of contraband.
16 This type of consumer is commonly referred to as a "seek and delete" offender, knowing
17 that the same or different contraband satisfying their interests remain easily discoverable
18 and accessible online for future viewing and self-gratification.

19 30. Based on my training and experience and my consultation with electronic
20 forensic detectives and agents who are familiar with searches of computers and smart
21 devices, I have learned that regardless of whether a person discards or collects depictions
22 of minors engaged in sexually explicit conduct he accesses for purposes of viewing and
23 sexual gratification, evidence of such activity is likely to be located. This evidence may
24 include the files themselves, logs of account access events, contact lists of others engaged
25 in trafficking of depictions of minors engaged in sexually explicit conduct, and other
26 electronic artifacts that may be forensically recoverable.

27 31. Based on my training and experience and my consultation with electronic
forensic detectives who are familiar with searches of smart devices, I have learned that
offenders will try and obfuscate data containing images and videos of minors engaged in

1 sexual activity. One potential manner of trying to hide the contraband may be by
2 changing file extensions. For example, an image file may often have a file extension of
3 “.jpg” or “.jpeg” signifying that it is an image or photograph. An offender may change
4 the that file extension by selecting the “save as” format on a computer or digital device
5 and select “.doc” or “.docx” to make it appear that instead of a contraband image or
6 photograph, it is a word document. The same process may be used to attempt to hide a
7 video file as well. Based on these and other attempts to hide potential contraband, it is
8 necessary for forensic examiners to examine all potential data on the computer.

9 32. Whether some data on the phone is evidence may depend on other
10 information stored on the computer, and the application of an examiner’s knowledge
11 about how a computer operates. Therefore, the context, location, and data surrounding
12 information in the computer’s data may be necessary to understand whether evidence
13 falls within the scope of the warrant.

14 33. I also know based on my training and experience that obtaining subscriber
15 information for a particular device is often useful in determining who possessed the
16 device on a particular date and time. However, a more definitive way to determine the
17 possessor of a device is to examine how the device is used over a period of days or
18 weeks. The content on the device itself, over a period of time, provides vital evidence of
19 the identity of the user of the device; such evidence can be found in communication
20 content, email information, linked social media accounts, photos (selfies), video, and any
21 location data on the device. Examination of all this data is necessary to accurately
22 determine who possessed the device at dates and times critical to the investigation.

23 34. I also know based on my training and experience that a search of the digital
24 device itself would irreversibly alter data and/or evidence on the device. The commonly
25 accepted best practice method to search a digital device for evidence involves creating a
26 digital image of the device and then searching that image for the responsive evidence.
27 Creating a forensic image does not alter any evidence on the device; it only copies the
data into a searchable format. The image is then searched using search tools to locate and

1 identify that evidence whose seizure is authorized by this warrant. The unaltered device
2 and the image are then preserved in evidence.

3 35. As set forth herein, I seek permission to search for and seize evidence,
4 fruits, and instrumentalities of the above-referenced crimes, and or things or data
5 identifying the individual engaged in the above referenced criminal activity, that might be
6 found in the SUBJECT DIGITAL DEVICES, in whatever form they are found. It has
7 been my experience that individuals involved and interested in depictions of minors
8 engaged in sexually explicit conduct often prefer to store images or videos depicting
9 depictions of minors engaged in sexually explicit conduct in electronic form. The ability
10 to store images of depictions of minors engaged in sexually explicit conduct in electronic
11 form makes digital devices an ideal repository for depictions of minors engaged in
sexually explicit conduct.

12 36. Based upon my knowledge, experience, and training in depictions of
13 minors engaged in sexually explicit conduct investigations, and the training and
14 experience of other law enforcement officers with whom I have had discussions, I know
15 that there are certain characteristics common to individuals with a sexual interest in
16 minors who are involved in depictions of minors engaged in sexually explicit conduct as
described below.

17 37. Those who possess, receive and attempt to receive depictions of minors
18 engaged in sexually explicit conduct may receive sexual gratification, stimulation, and
19 satisfaction from contact with children; or from fantasies they may have viewing children
20 engaged in sexual activity or in sexually suggestive poses, such as in person, in
21 photographs, or other visual media; or from literature describing such activity.
22 GILLETTE is a convicted sex offender with a prior Child Molestation First Degree
23 conviction involving a child who was 8 years old at the time of the offense thus
24 demonstrating a sexualized interest in minors prior DOC's most recent discovery of child
25 exploitation material as described above.

26 38. Those who possess, receive and attempt to receive depictions of minors
27 engaged in sexually explicit conduct may keep records, to include names, contact

1 information, and/or dates of their interaction, of the children they have attempted to
2 seduce, arouse, or with whom they have engaged in the desired sexual acts.

3 39. Those who possess, receive, and attempt to receive depictions of minors
4 engaged in sexually explicit conduct often maintain their collections that are in a digital
5 or electronic format in a safe, secure, and private environment, such as a computer and
6 surrounding area. These collections are often maintained for several years and are kept
7 close by, usually at the individual's residence, to enable the collector to view the
8 collection, which is valued highly. Again, GILLETTE is a convicted sex offender with a
9 prior Child Molestation First Degree conviction involving a child who was 8 years old at
10 the time of the offense thus demonstrating a sexualized interest in minors prior DOC's
11 most recent discovery of child exploitation material as described above.

12 40. Those who possess, receive and attempt to receive depictions of minors
13 engaged in sexually explicit conduct also may correspond with and/or meet others to
14 share information and materials; rarely destroy correspondence from other depictions of
15 minors engaged in sexually explicit conduct distributors/collectors; conceal such
16 correspondence as they do their sexually explicit material; and often maintain lists of
17 names, addresses, and telephone numbers of individuals with whom they have been in
18 contact and who share the same interests in depictions of minors engaged in sexually
19 explicit conduct.

20 41. Those who possess, receive, and attempt to receive depictions of minors
21 engaged in sexually explicit conduct prefer not to be without their depictions of minors
22 engaged in sexually explicit conduct for any prolonged time period. This behavior has
23 been documented by law enforcement officers involved in the investigation of depictions
24 of minors engaged in sexually explicit conduct throughout the world.

25 //

26 //

CONCLUSION

42. The affidavit and application are being presented by reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

43. Based on the information set forth herein, there is probable cause to search the above-described SUBJECT DIGITAL DEVICES, as further described in Attachment A, for evidence, fruits, and instrumentalities, as further described in Attachment B.

SHAFQAT M
MIRZA

Digitally signed by
SHAFQAT M MIRZA
Date: 2023.11.29 09:18:45
-08'00'

SHAFQAT MIRZA
special Agent
Homeland Security Investigations

SUBSCRIBED AND SWORN before me this 30th day of November, 2023


THE HON. PAULA L. MCCANDLIS
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant authorizes the seizure and search of SUBJECT DIGITAL DEVICES:

(1) a blue colored Samsung Galaxy S20, Model: SM-G781U;

(2) a black colored Samsung Galaxy S21, Model: SM-G990U; and

(3) a black colored Samsung Galaxy S9

and any other electronic storage media found therein the device including internal storage device cards which are currently located at Homeland Security Investigations secure evidence section.

ATTACHMENT B**Particular Things to be Seized**

The following items, which constitute fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2), including:

1. All records on the SUBJECT DIGITAL DEVICES described in Attachment A that relate to violations of Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2), including:

a. Evidence of other accounts associated with this device including email addresses, social media accounts, messaging “app” accounts, and other accounts that may be accessed through the digital device that will aid in determining the possessor/user of the device;

b. Evidence of use of the device to communicate with other individuals with a sexualized interest in minors or others about the above-listed crime(s), via incoming or outgoing calls, chat sessions, instant messages, text messages, app communications, social media, SMS communications, and other similar digital communications related to the sexual abuse of a minor or the possession or production of depictions of minors engaged in sexually explicit conduct;

c. Evidence of the identity of the person in possession of the device on or about any times that items of evidentiary value (user attribution evidence), located pursuant to this warrant, were created modified, accessed, or otherwise manipulated. Such evidence may be found in digital communications, photos and video and associated metadata, documents, social media activity, and electronically stored information from the digital device necessary to understand how the digital device was used, the purpose of its use, who used it, and when;

d. Child pornography as defined in 18 U.S.C. § 2256 meaning any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction

1 is a digital image, computer image, or computer-generated image that is, or is
2 indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the
3 visual depiction has been created, adapted, or modified to appear that an identifiable
4 minor is engaged in sexually explicit conduct), in any format or media;

5 e. Evidence of malware that would allow others to control the digital device
6 such as viruses, Trojan horses, and other forms of malicious software, as well as evidence
7 of the presence or absence of security software designed to detect malware; as well as
8 evidence of the lack of such malware;

9 f. Evidence of the attachment to the digital device of other storage devices or
10 similar containers for electronic evidence, and/or evidence that any of the digital devices
11 were attached to any other digital device;

12 g. Evidence of counter-forensic programs (and associated data) that are
13 designed to eliminate data from a digital device;

14 h. Evidence of times the digital device was used;

15 i. Electronically stored information from the SUBJECT DIGITAL DEVICE
16 necessary to understand how the digital device was used, the purpose of its use, who used
17 it, and when; and

18 j. Information that can be used to calculate the position of the SUBJECT
19 DEVICE, including location data; cell tower usage; GPS satellite data; GPS coordinates
20 for routes and destination queries between the above-listed dates; “app” data or usage
21 information and related location information; and images created, accessed or modified
22 between the above-listed dates, together with their metadata and EXIF tags.
23
24
25
26
27